CIS 700 Lecture 1: Intro + historical ciphers

(1)

Course Mechanics

- 30% HW (every ~2 weeks?)
- 30% midterm (tentatively November 17)
- 30% final project
- 10% intangibles

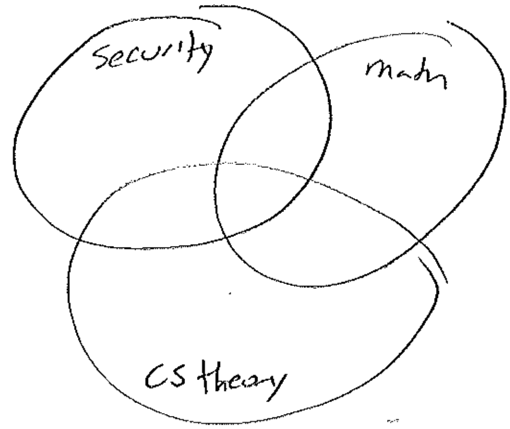
group work is ok
cite your sources + partners
write up separately
don't just divide up HW
single final project

NO TA - You will (communally) grade a HW.

OH: Tuesday 1:30 pm

Cryptography is...

- Part of (but not all) of security
- A fun application of math
- A fun sub-area of theoretical CS



Topics

- history (today)
- proper definitions + security reductions
- symmetric key crypto: stream ciphers, block ciphers
  PRGs PRFs
- integrity: MACS, hash functions
- public-key crypto: encryption, signatures
- fun topics: secret sharing, commitments, zero-knowledge proofs, lattices, cryptanalysis

Background:
relevant math: basic probability, little amount of algebra/number theory, reductions + proofs

coding: there will be coding

Historical Ciphers

Caesar Cipher 100-44 BC

plaintext	A B C D	. . . .	W X Y Z
shift	3 3 3 3		
ciphertext	D E F G		Z A B C

Augustus Caesar changed key from D to C
Generalization: shift cipher
Cryptanalysis:

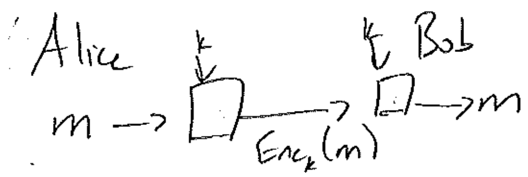
1. Brute force: only 26 possible keys
2. Frequency analysis: recognize letter distribution of English

Still in use!

2006: Mafia boss Bernardo Provenzano uses Caesar cipher (encoded w/ numbers)

2011: Rajib Karim plotted to blow up BA planes w/ Bangladeshi activists using Excel caesar cipher. (Rejected more modern crypto because "non-believers know about it so it must be less secure".)

Encryption Syntax:



Gen generate key k

Enc $c = Enc_k(m)$

Dec $m = Dec_k(c)$

satisfying $Dec_k(Enc_k(m)) = m$
"correctness"

Exercise: Formulate Caesar cipher.

Kerckhoff's Principle (Auguste Kerckhoff 1883)

"The cipher must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."

- encryption scheme should not be secret
- only key needs to be kept secret

Modern interpretation:

- Algorithms should be public, standardized, and scrutinized in public.

"Sufficient key space principle"

Any secure encryption scheme must have a key space that is not vulnerable to exhaustive search.

- necessary but not sufficient

Mono-alphabetic substitution

plain a b c d ...
cipher X E U A ...

what's # keys? ($26! \sim 2^{88}$)

How to break?

- Frequency analysis

Vigenère Cipher "poly-alphabetic shift"

Giovanni Batista Bellaso in 1553

ascribed to Blaise de Vigenère - French Diplomat

plaintext: TO BE OR NOT TO BE
key: run run run run r
cipher: K I O V I E E I G K I O V

Cryptanalysis:

If know key length n:

1. Break ciphertext into n
2. Solve each slice as a Caesar cipher

ciphertext-only attack
known-plaintext attack: trivially broken

How to find n?

Kasiski method (Friedrich Kasiski 1863)

Repeating strings eventually encrypted w/ same key letters

dist b/w repeated ciphertext strings prob. a mult. of key length

2009: Jacob Appelbaum finds circumvention tool Psiphon using a Vigenère cipher

psiphon.ca/node/25 "XOR cipher"

(fix still broken)

What if key is as long as plaintext? (And perfectly random)

One-Time Pad

Gen: $k \leftarrow_R \{0,1\}^\ell$ uniform

Enc: $k \in \{0,1\}^\ell$, $m \in \{0,1\}^\ell$ $\quad c = k \oplus m$

Dec: $m = c \oplus k$

What does "secure" mean?

1. No adversary can compute secret key from ciphertext?
2. No adversary can compute plaintext from ciphertext?
3. No adversary can determine a character of plaintext?
4. Meaningful information?
5. Can't compute any function of plaintext from ciphertext.

<u>Def</u> "perfect secrecy"

for every probability distribution over $\{m\}$

$\forall m \in \{m\}$ $\forall c \in \{c\}$

$Pr[M=m \mid C=c] = Pr[M=m]$ $\quad$ equivalently $Pr[C=c \mid M=m] = Pr[C=c]$

<u>Lemma</u> "perfect indistinguishability" $\qquad$ ciphertext-only attack

an encryption scheme is perfectly secret $\Leftrightarrow$

for every probability distribution over $\{m\}$

$\forall m_0, m_1 \in \{m\}$ $\forall c \in \{c\}$

$Pr[C=c \mid M=m_0] = Pr[C=c \mid M=m_1]$

<u>Proof</u> $\Rightarrow$: $Pr[C=c \mid M=m_0] = Pr[C=c] = Pr[C=c \mid M=m_1]$ ✓

$\Leftarrow$ Fix prob. dist. over $\{m\}$, arbitrary m_0, c

$$Pr[C=c] = \sum_m Pr[C=c \mid M=m] \cdot Pr[M=m]$$
$$= \sum_m Pr[C=c \mid M=m_0] \cdot Pr[M=m]$$
$$= Pr[C=c \mid M=m_0] \cdot \sum_m Pr[M=m]$$
$$= Pr[C=c \mid M=m_0] \quad \text{true for any } m_0 \checkmark$$

<u>Thm</u> OTP is perfectly secret

$Pr[C=c \mid M=m] = Pr[M \oplus k = c \mid M=m] = Pr[m \oplus k = c] = Pr[k = m \oplus c] = \frac{1}{2^\ell}$

$\Rightarrow$ for any m_0, m_1, $Pr[C=c \mid M=m_0] = \frac{1}{2^\ell} = Pr[C=c \mid M=m_1]$

<u>Thm</u> Let (Gen, Enc, Dec) be a perfectly secret encryption scheme
$\Rightarrow |\mathcal{K}| \geq |\mathcal{M}| \quad \mathcal{K} = \{k\} \quad \mathcal{M} = \{m\}$

<u>Pf</u> Show if $|\mathcal{K}| < |\mathcal{M}| \Rightarrow$ not perfectly secret.

Fix uniform distribution over $\mathcal{M}$.

Let $\mathcal{M}(c) = \{m \mid m = Dec_k(c) \text{ for some } k \in \mathcal{K}\}$

$|\mathcal{M}(c)| \leq |\mathcal{K}| \Rightarrow \exists\ m' \in \mathcal{M}$ s.t. $m' \notin \mathcal{M}(c)$

$Pr[M = m' \mid C = c] = 0 \neq Pr[M = m']$